International Journal of Computing and Network Technology
ISSN 2210-1519
Int. J. Com. Net. Teach. 3, No. 1 (Jan. 2015)

Utilizations of Reversible Lossless Data Hiding Techniques in Video Sequences

Osama F. Abdel Wahab[1], Mohamed B. Badawy[1], Osama A. Elshakankiry[1], Hala S. El-sayed[2]

[1]*Faculty of Electronic Engineering, Computer Science and Engineering Dep.,Menoufiya University,Minuf, Egypt.*
[2]*Faculty of Engineering, Electrical Engineering Dep.,Menoufiya University, Shebin El-Kom, Egypt.*

Received: 22 Sept, 2014, Revised: 5 Dec. 2014, Accepted: 15 Dec. 2014, Published: 1 Jan. 2015

Abstract: This paper propose a method of hiding data in selected video sequence. The proposed algorithm is a hybrid hiding scheme based on discrete wavelet transform (DWT) and histogram shifting for lossless data hiding . In this algorithm, First pre-processes the video sequence and frame conversion is to be done, the secret message is not embedded directly on the wavelet coefficients but by shifting parts of histogram of high frequency subbands to make space for data hiding and Finally, the secret message is extracted from the stego-video.This technique satisfy both imperceptibility and robustness. Experimental results show that this scheme outperforms the prior arts in terms of a larger payload (at the same PSNR) or a higher PSNR (at the same payload).

Keywords: Steganography, stego-image, stego-video, secret message, Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), Discrete Wavelet Transform (DWT), Integer Wavelet Transform (IWT).

1. INTRODUCTION

The development of information technologies makes it convenient for people to transmit mass data through Internet. However, it also provides vast opportunities for hackers to steal valuable information. Therefore, security becomes an important issue. Digital data hiding can hide sensitive information into multimedia for covert communications. Most multimedia data hiding techniques will distort the cover media in order to insert the additional information. Although the distortion is often small and imperceptible to human visual systems (HVS), the irreversibility is not admissible to some sensitive applications, such as legal and medical imaging. For these applications, lossless data hiding is desired to extract the embedded data as well as recover the original host signal.

By using lossless steganography techniques messages can be sent and received securely. Traditionally, steganography was based on hiding secret information in image files[1]. Lately, there has been growing interest applying steganographic techniques to video files as well [2]. The advantage of using video files in hiding information is the added security against hacker attacks due to the relative complexity of video compared to image files [2]. Image-based and video-based steganography techniques are mainly classified in to spatial domain and frequency domain based methods [3]. The former embeds messages directly in least Significant Bits (LSB) of the intensity of pixels of image or video. Spatial domain techniques either operate on pixel wise or block wise bases, these algorithms are characterized by the ability of high storage of data (payload) but they can't resist hacking. In frequency domain, images are first transformed to frequency domain e.g. by using FFT, DCT or DWT and then the messages are embedded in some or all of the transformed coefficients , these algorithms are characterized by resisting hacking , but it can't hide much data [2].

A lot of lossless data hiding methods have been developed. For a survey, readers are referred to [4]. Osama Fouad et al. [5] have proposed steganography algorithm based on color histograms for data embedding into Video to embed data in the spatial domain. Ni et al. [6] have proposed a histogram-manipulation based lossless data hiding scheme.Tian [7] embeds data using the difference expansion technique and results in one of the best reversible data hiding method among all the existing reversible data hiding techniques. Xuan et al. [8] proposed the reversible data hiding algorithms carried out in the integer wavelet transform (IWT) domain. One method losslessly compresses one or more than one middle bit-planes to save space for data embedding. Another applies spread-spectrum technique to embed data in high frequency IWT coefficients.

Most of the methods based on DWT have been designed to achieve two goals; to ensure confidentiality of data and to allow hiding the largest possible payload. However, in conventional wavelet transform,

E-mail address:osamaf@hotmail.com, mbmbadawy@yahoo.com, elshakankiry75@yahoo.com, hall_hhh@yahoo.com.

reversibility may not be achieved due to the loss of floating point accuracy of reversed wavelet coefficients. So, several methods of lossless data hiding [9, 10] overcome the above problem by using an invertible integer-to-integer wavelet transform. It maps integers to integers which are preserved in both forward and reverse transforms. Therefore, there is no loss of information. Jinna and Ganesan [10] shifted part of the histogram of integer-to-integer wavelet transformed coefficients to create space for embedding secret information bits.

In this paper, we focus on frequency domain technique. The DWT has received considerable attention in various signal processing applications, including image watermarking. The main idea behind DWT results from multi resolution analysis. This involves decomposition of an image in frequency channels of constant bandwidth on a logarithmic scale. The DWT can be implemented as a multistage transformation. An image is decomposed in to four sub bands denoted LL, LH, HL and HH at level 1 in the DWT domain, where LH, HL and HH represent the finest scale wavelet coefficients and LL stands for the coarse-level coefficients.

A. Basic Model

The basic model of proposed algorithm as shown in Fig.1 uses a cover Video (It used to hold secret data inside), the secret message (the secret data that is to be sent) and an embedding algorithm/technique (the procedure to hide secret message inside cover Video). The result of the process is the stego-video which is the digital video that has the secret message hidden inside. Stego-video is sent to the receiver via public communication channel where receiver will get the secret data out from the stego-video by applying an extracting algorithm/technique .

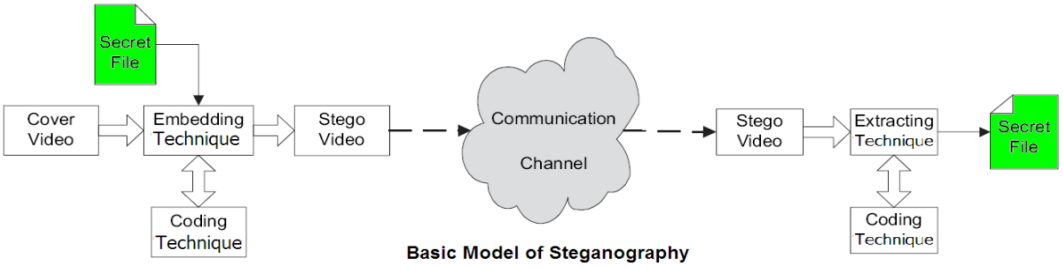


Fig.1: Basic Model

Table 1 – bit Distribution of 16-bit digital image

Bit	15	14	13	12	11	10	09	08	07	06	05	04	03	02	01	00
Color	**R**	**R**	**R**	**R**	**R**	**G**	**G**	**G**	**G**	**G**	**G**	**B**	**B**	**B**	**B**	**B**

B. Digital video basics

A digital video consists of a set of frames (images) that are played back at certain frame rates based on the video standards. Quality of the digital video depends on a set of parameters such as the number of pixels in a frame, the fps (frames per second), and frame size .The fps parameter is almost standard (between 24 and 30 fps) in many common video formats, however, the other two parameters present several altered from one video standard to another. Each image, which is called a frame, consists of pixels having three or four color compounds such as RGB (Red–Green–Blue) or CMYK (Cyan–Magenta–Yellow–Black). The rest of the intercessor colors are composed from a mixture of these primary colors [11]. Since the human eye is principally sensitive to green color tones, in some video standards the number of bits of each color compound may differ. For example, the red and blue colors are encoded in 5 bits while the green color consists of 6 bits for 16-bit color standard as seen in Table 1. In 24-bit RGB color, each red, green, and blue component is 8 bits long and has 256 variants in color density. In the CMYK standard on the other hand, 32-bit is needed and this standard is ordinarily used in modern computer displays [12].

Several researchers have addressed the problem of video steganography. In [2] a comparative analysis between Joint Picture Expert Group (JPEG) stego-image and Audio Video Interleaved (AVI) stego-video by quality and size was performed. The work presented in this paper is based on frequency domain processing of AVI video files as covert video. Data hiding mechanism provides imperceptibility and robustness.

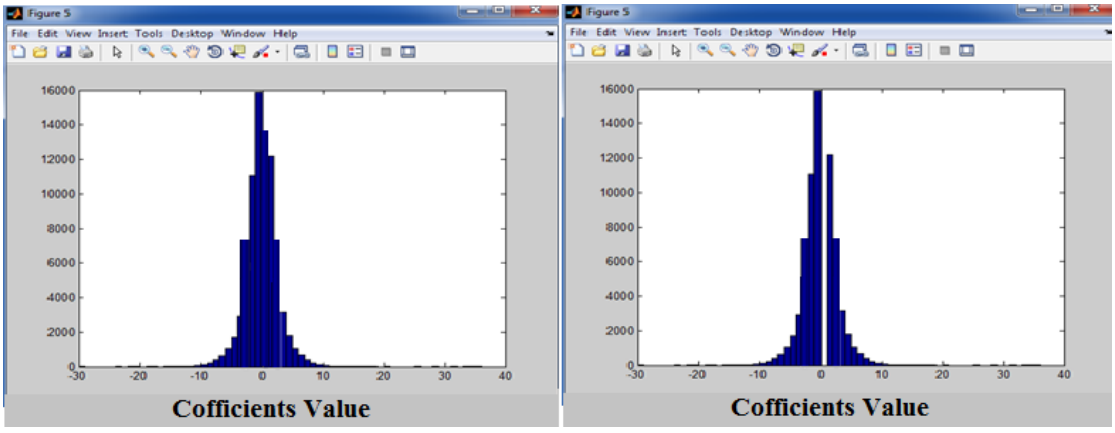
C. Video/Image Steganography

As we declared previously, A digital video consists of a set of frames (digital images) that are played back at certain frame rates based on the video standards. The image is a collection of pixels where each pixel is a combination of three colors RGB (Red, Green and Blue). The color of pixel dependent on the numeric value of

related with each color. Pixels in the image are displayed row by row horizontally. When data is hidden in the video/images, Stego-video get less troubled as compared to other multimedia files. After hiding data in an image, size of the image increases so compression techniques are necessary. When data is hidden in large size image, the transmission of video/image over the Internet takes more time and needs higher bandwidth. The size of the video/image can be reduced by compression technique. Compression techniques are grouped into two types, lossy and lossless. There are some of coding techniques are used to hide data in an image and video , we are going to discuss some of them below [9,10].

1. Integer-To-Integer Wavelet Transforms

In conventional wavelet transform reversibility is not achieved due to the floating point wavelet coefficients we can get after transformation. When we take the inverse transform the original pixel values will get altered. When we transform an image block consisting of integer-valued pixels into wavelet domain using a floating-point wavelet transform and the values of the wavelet coefficients are changed during secret message embedding, the corresponding stego-image block will not have integer values. When we truncate the floating point values of the pixels, it may result in loss of information and reversibility is lost. The original image cannot be reconstructed from the stego-image.In conventional wavelet transform done as a floating-point transform followed by a truncation or rounding it is impossible to represent transform coefficients accurately. Information will be potentially lost through forward and inverse transforms. In view of the above problems, an invertible integer-to-integer wavelet transform based on lifting is used in the proposed scheme. It maps integers to integers which are preserved in both forward and reverse transforms. There is no loss of information. Wavelet or sub band decomposition associated with finite length filters is obtained by a finite number of primal and dual lifting followed by scaling.



(a) **(b)**

Figure 2: Illustration of Wavelet Histogram, (a) Maximum Point is at Peak, (b) Histogram with Zero Point Created at Peak +1 (Jinna & Ganesan [10], 2010)

2. Wavelet Histogram Shifting

Integer Wavelet transforms of the original image is taken. In the sub band wavelet histogram data is to be embedded. In the histogram the horizontal axis (X) represents the wavelet coefficients value and the vertical axis (Y) represents the number of occurrence of each coefficient's value. The wavelet histogram normally exhibits a Laplacian distribution nature with a peak point and sloping on either side. Peak in wavelet histogram is usually at coefficient value '0'. Embedding can be done on both the sides of the histogram to get the required embedding capacity. Data embedding is done by modifying some of the coefficient values of the wavelet domain to its neighboring value by shifting a portion of the histogram. This gives a good visual quality and thereby a better PSNR between original image and stego-image.

To embed data we choose the peak point of the histogram and call it as P. Figure 2 shows a vacant point is created at Peak+1.This is done by shifting all points with value Peak+1 and above one position to the right. Now all the IWT coefficients are scanned and whenever a coefficient with value peak is encountered, '0' is embedded by leaving it as such and '1' is embedded by changing its value to peak+1.This is repeated till all the points with value Peak are over. Then a new peak is created by shifting to the right and data is embedded as per the algorithm. We choose the peak point so that payload is maximized.

All the high frequency wavelet sub bands can be utilized to get maximum capacity. The same process can be done on the left side of the histogram Peak to embed more secret bits. A reverse algorithm is applied for extracting the secret data.

After water mark bits are extracted, shifting is done towards the left each time after data extraction so that the original coefficient values are restored. This guarantees complete reversibility and the original image can be exactly reconstructed without loss.

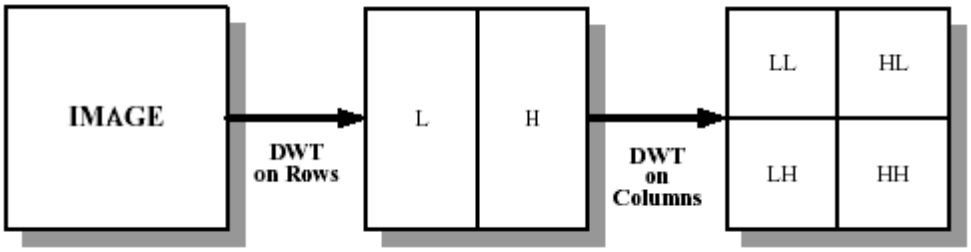


Figure 3:Block Diagram of DWT (a) Original Image **(b) Output image after the first 1-D applied on Row input** **(c) Output image after the second 1-D applied on row input.**

3. Discrete wavelet transform

Wavelets are special functions which, in a form analogous to sines and cosines in Fourier analysis, are used as basal functions for representing signals. For images, applying DWT corresponds to processing the image by filters in each dimension. The filters divide the input image into four non-overlapping multi-resolution sub-bands LL1, LH1, HL1 and HH1. The sub-band LL1 represents the coarse-scale DWT coefficients while the sub-bands LH1, HL1 and HH1 represent the fine-scale of DWT coefficients. To obtain the next coarser scale of wavelet coefficients, the sub-band LL1 is further processed until some final scale N is reached. When N is reached, 3N+1 sub-bands consisting of the multiresolution sub-bands LLx and LHx, HLx and HHx is obtained where x ranges from 1 until N.

Due to its excellent spatial-frequency localization properties, the DWT is very suitable to identify the areas in the host image where secret message can be embedded effectively. In particular, this property allows the exploitation of the masking effect of the human visual system such that if a DWT coefficient is modified, only the region to that coefficient will be modified. In general, most of the image energy is concentrated at the lower frequency sub-bands LLx and therefore embedding secret message in these sub-bands may degrade the image significantly. Embedding in the low frequency sub bands however, could increase robustness significantly.

On the other hand, the high frequency sub-bands HHx include the edges and textures of the image and the human eye is not generally sensitive to changes in such sub-bands. This allows the secret message to be embedded without being perceived by the human eye. The compromise adopted by many DWT based algorithm, is to be embed the secret message in the middle frequency sub-bands LHx and HLx where acceptable performance of imperceptibility and robustness could be achieved. Wavelet transform decomposes a signal into a set of a basis functions. These basis functions are called wavelets. Wavelets are obtained from a single prototype wavelet y(t): Called mother wavelet by dilations and shifting $\Psi_{a,b}(t) = |a|^{-\frac{1}{2}} \Psi\left(\frac{t-b}{a}\right)$.Where a and b are the scaling and shifting parameters, respectively.

This paper is ordered as follows. Section II, we discuss the relevant research work of Wavelet Transform, Histogram Shifting and the histogram-based data hiding approaches. Section III, describes our proposed method. Section IV demonstrates the experimental results, and conclusions are given in Section V.

2. RELATED WORK

Jinna and Ganesan [10] proposed a method of lossless data hiding in images using integer wavelet transform IWT and histogram shifting The method shifts part of the histogram to create space for embedding the secret information bits. The method embeds secret message while maintaining the visual quality well. The method is completely reversible. The original image and the secret data can be recovered without any loss.

A. Hamsathvani [13] proposed hybrid image-hiding scheme based on discrete wavelet transform (DWT) and singular value decomposition (SVD) , the secret image is not embedded directly on the wavelet coefficients but rather than on the elements of singular values of the cover image's DWT sub bands and also find the SVD of the cover image or each block of the cover image, and then modify the singular values to embed the secret message. MSE is calculated for each frame and then embed the secret message which has low MSE. Finally, the secret image is extracted from the stego-image. These techniques satisfy both imperceptibility and robustness.

Lin et al. [14] studied a several of schemes by which the histogram was constructed using a difference image to realize the task of reversible data hiding. The aim of this treatment was to present a more centralized histogram, which in turn may raise the heights of peak points and thus improve the capacity upon the histogram-based methods.

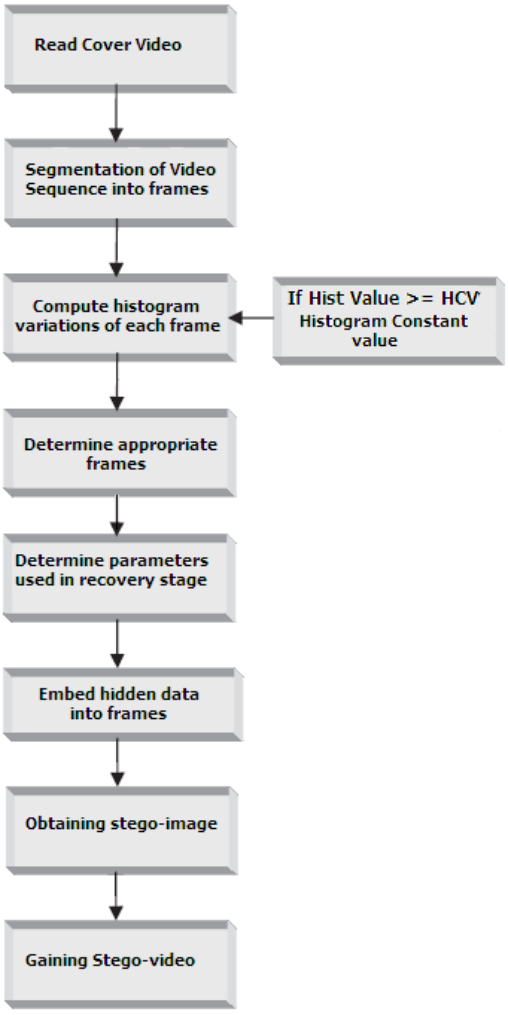


Fig. 4: Flowchart of embedding Algorithm

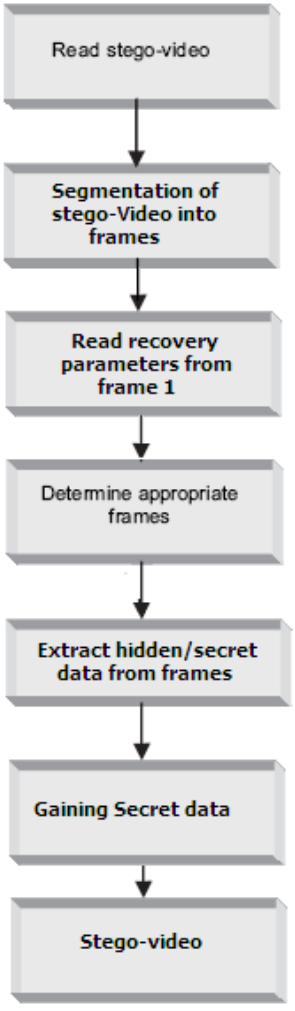


Fig. 5: Flowchart of extracting Algorithm

Yang et al. [15] proposed a new scheme utilizing column-based interleaving predictions to enhance the performance of Lin et al.'s histogram-based method.

The embedding capacity can be mostly increased by raising the heights of peak points in the histogram. Moreover, the difference between the original and updated values of each pixel remains within small rang after secret data embedding and the peak signal-to-noise ratio (PSNR) of the stego-image in each video frame is above 47 dB.

The proposed lossless data hiding technique is rather simple and, outperforms the prior arts. Both theoretical analysis and experimental results demonstrate the superiority of the proposed technique.

3. ALGORITHIM

In proposed algorithm the cover video segmented into frames and the histogram values of each frame are calculated. First, an calculating value is computed using the color and motion transitions in each frame by our application MATLAB software that we have developed. A predefined threshold value controlled by a track bar control on the software user interface. The threshold value, which can be as much as the highest pixel number of the video frame, indicates a certain level of disparity between successive video frames. Histogram variations of consecutive video frames are compared to the threshold value (Histogram constant Value HCV) and appropriate pixels in those frames are selected for data embedding procedures, the higher the threshold values are the more the perceptibility precision is increased at frame transitions in contrast to a decrease in the number of segmented frames. This consequently means a capacity drop for the embedded data. If the threshold value is configured as low, parameter values mentioned above will be inverse [5].The detail of the embedding and extracting algorithms are shown in the following subsections.

A. Video's Segmentation and select frames

The data hiding method is initiated by segmentation of cover-video file into the frames, the average histogram values of frames are calculated and appropriate frames are determined in respect to the HCV parameter. The flowchart of our proposed scheme is shown in Fig. 4 and Fig. 5.

B. Embedding Algorithm

The flowchart is shown in Fig.4.

Input: Secret message, original selected frames of cover video

For the wavelet transformed image subbands histogram is taken. Now we can start embedding using the following steps. For the selected sub band, set P = Peak of the histogram coefficients.

Create a zero point at P+1 so that no point in the histogram has the value P+1.To create the zero point shift all coefficients with value P+1and above to one position right. This makes P+1 as P+2, and the original P+2 to P+3 and so on.

1. Now positions P and P+1 are chosen to embed data.

2. Read the (n) secret message bits (W_b) where $0 < b < n-1$.

3. Check $W_b = 0$, then '0' is embedded in the coefficient with value P by leaving it unchanged as P.

4. Check $W_b = 1$, then '1' is embedded in the coefficient with value P by changing it to value P+1.

5. Point P+1 gets slowly filled up depending upon the number of (W_b) bits with value 1.

6. Go to histogram of the other sub bands to be marked and repeat the same process.

7. if embedded secret message bits are still remaining , set P=Peak+2 and go to step1. Otherwise stop.

The original image in selected frames is decomposed into its sub bands using integer wavelet transform After preprocessing IWT is used to ensure complete reversibility.

The high frequency sub bands (horizontal, Vertical and Diagonal) are used for data embedding. Each sub band is used one after the other to meet the required embedding capacity. Secret message bits that forms the payload is embedded into these sub bands using the embedding algorithm. The low frequency unmarked approximate coefficients are then used along with the marked sub bands and Inverse IWT is taken to get the Stego-image.

Output : Stego-image , stego-video

C. Extracting Algorithm

The flowchart is shown in Fig. 5.

Input : Stego-video, Stego-image for selected frames of Stego-video

Data extraction is the reverse process. Integer wavelet Transform is taken for the Stego-image. The Stego-image high frequency sub bands are separated and using the Data extraction algorithm, the secret message bits are retrieved and the original sub bands are obtained. This is combined with the unmarked low frequency sub band to get the original image. This method is completely blind and reversible. Original image and the secret message bits are obtained without any loss.

After wavelet decomposition of the stego-image, histograms of the marked sub bands are taken. For the selected sub band, set Peak= Peak of the histogram coefficients.

1. P =Peak. Read the coefficients with value P and P+1. Whenever a coefficient with value P is read ,extract secret bit as $W_b = 0$ and leave P unaltered. Whenever a coefficient with value P+1 is read ,extract secret bit as $W_b = 1$ and change P+1 to P.

2. Shift all the coefficients with value P+2 and above one position to the left.

3. Go to histogram of the other marked sub bands and repeat the same process.

4. Set P = Peak+1.

5. While all secret message bits (W_b) are not extracted go to step1.Otherwise stop.

Output: Secret message, stego-video .

Table 2: The number of faded pixels in varied coding techniques

Cover video size (byte)	Hiding file size (byte)	Faded pixels in cover video					
		proposed Algorithm		Previous Algorithm		LSB coding	RGB coding
		coding	PSNR	coding	PSNR		
'vipmen.avi ' 1,522,0624	73	65	48.85	69	47.91	195	73
	1800	1624	48.76	1710	48.11	4800	1800
	27,648	24,951	48.75	26,265	48.32	73,728	27,648
	46,080	41,587	48.70	43,776	48.40	122,880	46,080
	54,784	49,441	48.10	52,044	48.45	146,091	54,784
	103,424	93,339	47.80	98,252	48.56	275,798	103,424
	145,408	131,230	46.52	138,137	48.81	387,755	145,408
	168,960	152,486	42.12	160,512	48.84	450,560	168,960

4. EXPERIMENTAL RESULTS

Steganography is characterized mainly by two aspects; imperceptibility and robustness. Imperceptibility means the embedded data must be imperceptible to the observer (perceptual invisibility) and computer analysis (statistical invisibility). Robustness means capacity (maximum payload is required) i.e., maximum amount of data that can be embedded into the cover image without losing fidelity of the original image [17].

The perceptual imperceptibility of the embedded image is indicated by comparing the original image or video to its stego counterpart so that their visual differences, if any, can be determined. Additionally, as an objective measure Peak Signal to Noise Ratio may be calculated. It is the ratio between a signal's maximum power and the power of the signal's noise.

Engineers commonly use the PSNR to measure the quality of reconstructed signals that have been compressed. Signals can have a wide dynamic range, so PSNR is usually expressed in decibels, which is a logarithmic scale.

In this section, we report the experimental results comparing proposed method with Osama Fouad et al. [5] our Previous Algorithm and the O.CETIIN et al. [16] schemes. To show the performance of the proposed method, we implement the schemas shown by O.CETIIN et al. [16] , our Previous Algorithm and the proposed method in this paper are using MATLAB software. The embedded secret message was generated by repeat a predefine message until embedded message with required length is generated. We used 'scenevideoclip.avi' and 'vipmen.avi' as test cover video file from under MATLAB software toolbox folder. We used PSNR (peak signal to noise ratio) to measure the distortion between the original video and Stego-video.

The proposed algorithm able to hide messages within part of the frames or the whole Frames based on HCV value and the random selection of frames and pixels increases the level of security to hide and extract the secret messages.

The obtained outcomes are shown in Table 2. From the obtained results we can conclude that the embedding capacity in the proposed algorithm is very good. also, the PSNR in the table shows that the image quality is very good and has higher level of security as compared to other algorithms.

5. CONCLUSION

In this paper, the goal of the proposed algorithm is to decrease the faded pixels in each frame, in order to increase the embedding capacity. The experimental outcomes showed that the proposed algorithm is improve the embedding capacity, maintains the quality of the stego-video, more efficient, simple, appropriate and accurate than other algorithms, as well as it makes the secret message more secure.

REFERENCES

[1] N. Provos and P. Honeyman, "Hide and Seek: An Introduction to Steganography", IEEE Security & Privacy Magazine, Vol. 1, issue 3, pp. 32-44, June 2003.

[2] R.Kavitha and A. Murugan, "Lossless Steganography on AVI File using Swapping Algorithm", International Conference on Computational Intelligence and Multimedia Applications, pp. 83-88, Sivakasi-TamilNadu, Dec. 2007.

[3] C. Ming, Z. Ru, N. Xinxin and Y. Yixian, "Analysis of Current Steganography Tools: Classifications &Features", Proceedings of the 2006 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06), pp. 384-387, California, Dec. 2006.

[4] Y. Q. Shi, "Reversible data hiding," Proceedings of International Workshop on Digital Watermarking, Seoul, Korea, Oct. 1 to Nov. 2, 2004.

[5] Kelash H.M., Osama Fouad , Elshakankiry O.A. and El-sayed H.S. 'Hiding Data in Video Sequences Using Steganography Algorithms', ICT International Conference (ICTC 2013) , IEEE, pp. 353-358 , 10.1109/ICTC.2013.6675372 , Jeju Island , Korea, 14-16 Oct. 2013.

[6] Z. Ni, Y. Q. Shi, N. Ansari and W. Su, "Reversible data hiding," Proceedings of IEEE International Symposium on Circuits and Systems, vol. 2, pp. 912-915, Bangkok, Thailand, May 2003.

[7] J. Tian, "Reversible data embedding using a difference expansion," IEEE Transactions on Circuits and Systems for Video Technology, pp. 890-896, Aug. 2003.

[8] G. Xuan, Y. Q. Shi, Z. Ni, "Lossless data hiding using integer wavelet transform and spread spectrum," IEEE International Workshop on Multimedia Signal Processing,Siena, Italy, September 2004.

[9] G. Xuan, Y. Shi, C. Yang, Y. Zheng, D. Zou, and P. Chai, "Lossless Data Hiding Using Integer Wavelet Transform and Threshold Embedding Technique," Multimedia and Expo, ICME, IEEE International Conference, 2005, pp. 1520–1523.

[10] L. Ganesan, and S. Jinna, "Reversible Image Data Hiding Using Lifting Wavelet Transform and Histogram Shifting," International Journal of Computer Science and Information Security, Vol. 7, No. 3, 2010, pp. 283–290.

[11] Chincholkar A.A. and Urkude D.A., "Design and Implementation of Image Steganography", Journal of Signal and Image Processing, ISSN: 0976-8882 & E-ISSN: 0976-8890, Volume 3, Issue 3, pp. 111-113, 2012.

[12] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad and Osamah M. Al - Qershi, "Image Steganography Techniques : an Overview", International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue(3) : 2012.

[13] A. Hamsathvani "Image Hiding in Video Sequence Based On MSE", IJECSE,Volume1,Number 3 , 2012 , pp.1489-1493 , ISSN 2277-1956/V1N3-1489-1493 .

[14] Lin C.C., Tai W.L., and Chang C.C.: `Multilevel reversible data hiding based on histogram modification ofdifference images', Pattern Recognition, 2008, 41, pp. 3582-3591.

[15] Yang C.H., and Tsai M.H.: `Improving Histogram-based Reversible Data Hiding by Interleaving Predictions', IET Image Processing, 2010, 4, pp. 223-234.

[16] O.CETIIN and A.OZCERIT, "A new Steganography Algorithm Based on Color Histograms for Data Embedding into Raw Video Streams", Elsevier Ltd ,Computers & Security, Sakarya University, Turkey,Vol.28, pp. 670-682 , 2009.

[17] Venkatraman S., Ajith Abraham and Marcin Paprzycki, "Significance of Steganography on Data Security", International Conference on Information Technology: Coding and Computing (ITCC'04), Vol. 2, April 2004.

Osama Fouad Abdel Wahab

Received BSc.Eng.in Computer Science & EngineeringfromFaculty of ElectronicEngineering, Menoufiya University, Minuf, Egypt in 1991 and a M.Sc. in Computer Science & Engineering from Faculty of Electronic Engineering in 2014,He is currently working as a ICT consultant and a Lecturer at Kuwait University. His research topics include information,Network, Internet and Multimedia Security, Cryptography, Steganography and steganographic algorithms for video applications. Email: osamaf@hotmail.com

Osama A. Elshakankiry

Received a B.S. in Computer Science & Engineering from Faculty of Electronic Engineering, Menoufiya University, Egypt in 1998, a M.Sc. in Computer Science &Engineering from Faculty of Electronic Engineering, Menoufiya University, Egypt in 2003, and a Ph.D. in Computer Science from School of Computer Science, Faculty of Engineering and Physical Sciences, University of Manchester, UK in 2010. He was appointed as a demonstrator at the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, from 1999 to 2003. He became an assistant Lecturer in 2003 and promoted to a Lecturer in 2011. His research interests cover Network Security, Internet Security, Multimedia Security, Cryptography, and Steganography.

Mohammed Badawy

Received his B.Sc. and M.S. in computer science and engineering at Menoufiya University (Egypt) and received his Ph.D. in computer science and engineering at Czech Technical University in Prague (Czech Republic). He worked as assistant professor in the department of Computer Science and Engineering at Menoufia University (Egypt) from 2002 to 2005. He worked as assistant professor in the department of Information Technology at Taif University (KSA) from 2005 to 2010 (3 years of them as chairman of the department). Then he worked as an assistant professor in the College of Computers and Information Technology at Islamic University (KSA) from 2010 to 2013. Currently, he works as assistant professor in the department of Computer Engineering and Science at the Faculty of Electronic Engineering, Menoufia University (EGYPT). He is a member of Association of Computer Science and Information Technology (IACSIT). He is a reviewer of the International Journal of Engineering and Technology (IJET), King Abdul-Aziz City for Science and Technology (KACST)(KSA), Taif University research projects (KSA), and Northern Border University research projects(KSA). His research interests include databases, data stream systems, data mining, and software development. He has published about 14 papers in various scientific journals and refereed conferences. mbmbadawy@yahoo.com

Hala S. El-sayed

Received the B.Sc., M.Sc., and Ph.D. degrees in electrical engineering from Menoufiya University, Shebin El-kom, Egypt, in 2000, 2004, and 2010, respectively. She is currently with the Department of Electrical Engineering, Faculty of Engineering, Menoufia University, where she was a Demonstrator from 2002 to 2004 and has been a Lecturer since 2010. Her research interests cover Network security, Wireless sensor network, Secure building automation systems, and Biometrics.